Ciberseguridad en redes IEC 61850: Cómo Mitigación de vulnerabilidades de la mensajería GOOSE

Mauricio Gadelha da Silveira y Paulo Henrique Franco, Schweitzer Engineering Laboratories, Inc.

Resumen —IEC 61850 es un estándar utilizado para organizar el flujo de información dentro de una SE (Subestación Eléctrica) a través de protocolos de comunicación no propietarios. Los mensajes GOOSE están diseñados para viajar en la capa de enlace de datos del modelo OSI. Debido a la necesidad de alta

En el rendimiento del intercambio de información, los mensajes se ven privados de procedimientos de seguridad como la autenticación del editor y el cifrado de mensajes. Este trabajo explora las debilidades implícitas en los mensajes GOOSE (Generic Object Oriented Substation Event) y las formas de mitigarlas mediante el uso de conmutadores administrados y redes definidas por software (SDN).

Palabras clave: IEC 61850, GOOSE, ciberseguridad, SDN.

I. INTRODUCCIÓN

Durante mucho tiempo, las subestaciones eléctricas operaron sus esquemas de control y protección a través de cables de control, conjuntos de contactos y protocolos de comunicación propietarios (Dolezilek, Whitehead y Skendzik, 2010). Los avances en la tecnología de equipos de protección y control han permitido compartir información mediante cables y hardware de comunicación. Sin embargo, la estandarización de la información se hizo necesaria para el intercambio de información entre equipos de diferentes fabricantes. La norma IEC 61850 define globalmente cómo se debe construir, procesar y transmitir la información a través de la definición de una clase común de datos que permite la construcción de una semántica definida (Ozansoy, 2010), (IEC 61850-7-1, 2003), y puede ser transmitida de forma vertical u horizontal.

La comunicación vertical, de tipo cliente-servidor, que conecta los equipos al sistema SCADA se implementa utilizando el estándar MMS (Manufacturing Message Specification) (O'Fallon, Klas, Tibbals, Shah, & S, 2013). El mecanismo de multidifusión, utilizado para el intercambio horizontal de mensajes entre IEDs (Intelligence Equipment Devices) se define a través del protocolo GOOSE (Generic Object Oriented Substation Event). Los mensajes GOOSE fueron diseñados para viajar en la capa de enlace de datos del modelo OSI y su implementación se describe en IEC 61850-8-1, (IEC 61850-8-1, 2004).

La necesidad de un alto rendimiento para el intercambio de mensajes entre IED requiere la abstracción de procedimientos de seguridad tales como: autenticación del editor y cifrado de mensajes. Técnicas de ataque como la saturación de la red y la manipulación de tramas Ethernet explotan esta debilidad y pueden utilizarse para impedir el correcto funcionamiento de los SE e incluso provocar operaciones incorrectas. La técnica de saturación de la red consiste en inundar la red con mensajes GOOSE con la misma semántica que el editor, lo que hace imposible procesar adecuadamente los mensajes reales enviados por el editor al dispositivo suscriptor. La técnica de manipulación de tramas de Ethernet tiene como objetivo identificar mensajes GOOSE y cambiar el valor de los datos de los mensajes, provocando que el dispositivo suscriptor descarte los mensajes reales posteriores del dispositivo editor o haga que el dispositivo suscriptor funcione incorrectamente.

Se utilizan las mejores prácticas de configuración de red para mitigar estas y otras formas de ataques que pueden ocurrir en las subestaciones eléctricas. Estas prácticas utilizan la correcta aplicación de Redes Virtuales (VLANs), bloqueo de puertos que no están en uso y nuevas tecnologías de gestión de redes definidas por software (SDN) a través del control del flujo de datos. Por lo tanto, estas técnicas de ataque aprovechan las brechas que se pueden encontrar en los sistemas de automatización de subestaciones y que se pueden prevenir con una correcta ingeniería de red dentro de la subestación, aumentando el rendimiento, la confiabilidad y la seguridad del sistema de automatización.

II. REVISIÓN BIBLIOGRÁFICA

A. Mensajes de GOOSE

Los mensajes GOOSE están diseñados para ser rápidos y proporcionar un mecanismo que permita el intercambio de información entre uno o más IED a través de una red IEEE 802.3. Los mensajes GOOSE se transmiten a través del mecanismo de multidifusión y se distribuyen a través de una configuración de publicador/suscriptor, donde un IED es responsable de crear mensajes (publicador) que se entregan a un grupo de IED suscriptores, como se muestra en la Fig.

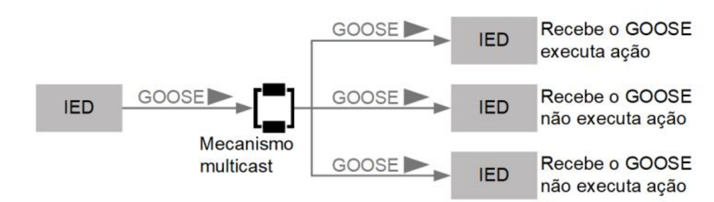


Figura 1. Mecanismo de multidifusión

La información sigue un datagrama descrito en IEC 61850-8-1 y se asigna a la capa de enlace de datos del modelo OSI, evitando sobrecargas de las capas adyacentes. Por lo tanto, no hay soporte para la autenticación de mensajes.

1) Estructura del datagrama GOOSE

Los mensajes GOOSE están diseñados y mapeados directamente en la capa de enlace de datos del modelo OSI y utilizan la arquitectura Ethernet para la construcción del marco, como se muestra en la Figura 2.

Preâmbulo	Início do quadro	Endereço MAC de destino	Endereço MAC de origem	Marcação IEEE 802.1 Q	Ethertype	APPID	Duração	Reservado 1	Reservado 2	APDU	Verificação do quadro

Figura 2. Datagrama GOOSE

Los campos Preámbulo e Inicio del marco son idénticos a los dos primeros campos del marco Ethernet. El campo de dirección MAC de destino corresponde a la dirección de multidifusión. IEC 61850 define un rango para direccionamiento de mensajes que comienza con los primeros tres octetos: 01-0C-CD. El cuarto octeto simboliza el tipo de datagrama, 01 para GOOSE, 02 para GSSE o 04 para SV. Los octetos quinto y sexto definen la dirección individual del mensaje.

El campo de dirección MAC de origen define la dirección de unidifusión del mensaje. Las etiquetas IEEE 802.1Q (etiquetado de prioridad de VLAN) (IEEE Std. 802.1Q, 2012) definen un mecanismo de selección y segregación de mensajes. El étertipo GOOSE se define como 88-B8. El APPID identifica el marco. El campo Longitud

Indica el número total de bytes en el mensaje. Los campos Reservado 1 y Reservado 2 están reservados para una futura estandarización. Los últimos campos son la APDU (Unidad de datos del protocolo de aplicación) y la comprobación secuencial de las tramas.

La carga útil es donde se encuentra la APDU que contiene la información que necesita ser compartida. Los datos contenidos en la APDU se codifican de acuerdo con los siguientes estándares: Notación de sintaxis abstracta uno / Regla de codificación básica (ASN.1/BER) (Kriger, Behardien y Retonda-Mo, 2013).

ASN.1 describe cómo debe verse la estructura de datos de una pieza de información. La sintaxis de los octetos de información que se transmitirán a través de un canal de comunicación en serie es responsabilidad de la codificación BER. La figura 3 muestra cómo se divide la información contenida en la APDU.

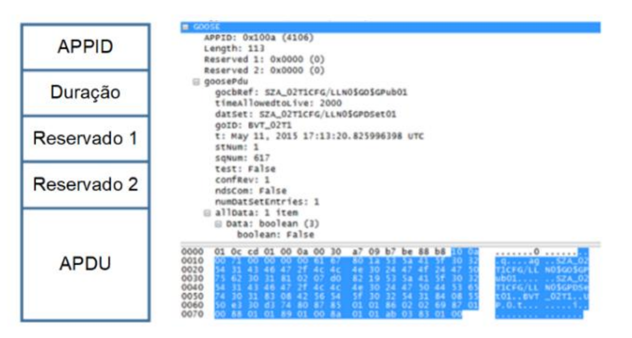


Figura 3. APDU de GOOSE

La APDU, descrita en el Anexo A de IEC 61850-8-1, es una secuencia de 11 parámetros que transportan la información que debe entregarse a los IED suscriptores. La información se divide en:

- gocbRef: Identificación única de la APDU que contiene el Dirección LN0
- TimeAllowedtoLive: informa al receptor del tiempo máximo de espera para la próxima retransmisión
- DatSet: Referencia de identificación del conjunto de datos
- goID: identificación del mensaje GOOSE
- t: marca de tiempo del mensaje
- stNum: State Number; Contador incrementado a cada disparador de nuevo mensaje
- sqNum: Número de secuencia ; Contador de retransmisión (se reinicia con cada nuevo evento activado)
- prueba: El parámetro de prueba indica si el mensaje está en modo de prueba
- confRev: Contador que se incrementa con cada cambio en la configuración del DataSet
- ndsCom: Necesita Puesta en Marcha, Parámetro utilizado para reportar posible falla en el mensaje o equipo
- numDatSetEntries: Número de elementos dentro del Conjunto de datos
- allData: Contiene la información LN almacenada por los DataSets

La información en el campo allData son contenedores (DataSets) que almacenan la información representada por los LN. La información contenida en los DataSets se codifica a través de los mecanismos descritos en IEC 61850 8-1 y se distribuye a través de una envolvente Ethernet (Konka, Arthur, Garcia, & Atkinson, 2011).

2) Dinámica de transmisión del mensaje GOOSE

El rendimiento de los mensajes GOOSE se describe en IEC 61850-5 (IEC 61850-5, 2003) y se clasifica como tipos 1 y 1A. Los mensajes de tipo 1 (mensajes rápidos) generalmente contienen contenido binario, pero pueden transportar cantidades analógicas. Los mensajes de tipo 1A son mensajes críticos en una subestación cuyos requisitos de rendimiento requieren una transmisión del orden de 3 ms en el caso más crítico.

Al generar un evento, el IED editor codifica la información contenida en el DataSet y la transmite a través del canal de comunicación a los receptores mediante una conexión multicast. La propagación de mensajes, definida en IEC 61850-8-1, tiene una dinámica de retransmisión de mensajes que se muestra en la Figura 4.

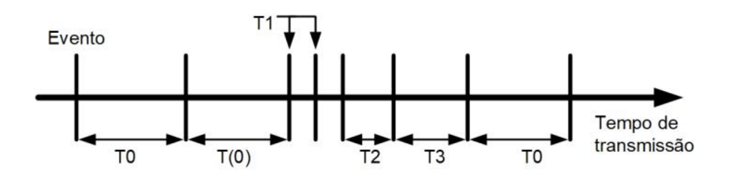


Fig. 4. Mecanismo de transmisión de mensajes GOOSE

Los eventos se generan en la aplicación IED local, se asignan en conjuntos de datos y se envuelven en mensajes GOOSE. Si no hay variación en las variables del contenedor allData , los mensajes viajan en régimen constante, periódicamente y respetando el tiempo de retransmisión T0.

La transición del estado de la información, representada por un LN, organizado en DataSets, desencadena el mecanismo de retransmisión rápida del mensaje GOOSE. El tiempo (T0) representa la transición del estado continuo al estado de retransmisión rápida. El tiempo T1 es la transmisión más rápida después de que ocurre un evento. Los tiempos T2 y T3 son los tiempos asociados a la recomposición de mensajes en régimen permanente. El tiempo y la forma de retransmisión T1 pueden variar según el tipo de fabricante.

Con cada transmisión de mensaje por parte del editor, el contador SqNum se incrementa hasta que se activa un nuevo evento, momento en el cual el contador se reinicia. El contador StNum se actualiza con cada nuevo evento. Los contadores SqNum y StNum están vinculados directamente al funcionamiento del motor de mensajes GOOSE. Variando los parámetros del contador es posible analizar el comportamiento de los mensajes GOOSE.

3) Vulnerabilidad de los mensajes GOOSE

Los mensajes GOOSE transportan información importante dentro de un SE. Las señales de apertura, cierre y TRIP suelen formar parte del alcance de los mensajes. Por lo tanto, los mensajes GOOSE influyen directamente en el comportamiento del SE. Sin embargo, los mensajes GOOSE y SV no implementan ninguna recomendación de seguridad a nivel de enlace en sus transmisiones de multidifusión.

La latencia introducida por el cifrado y la autenticación de mensajes es la principal barrera para la implementación a nivel de enlace. La norma IEC 62351 define métodos computacionales de bajo consumo, pero no son suficientes para cumplir con los requisitos de rendimiento exigidos por la norma IEC 61850-5 (Hoyos, Dehus y Brown, 2012). La norma IEC 61850-5 define un tiempo de transmisión mínimo de 3 ms para los mensajes de tipo 1 A que no pueden
se pueden cumplir utilizando métodos de seguridad a nivel de marco (cifrado y autenticación de mensajes). Por lo tanto, los mensajes GOOSE son inherentemente vulnerables debido a su diseño.

La vulnerabilidad se considera baja sólo para redes LAN aisladas sin comunicación con el mundo exterior. Dada la situación actual de los SE, donde la información se comparte con los centros de operaciones a través de gateways y enlaces de comunicación compartidos, ya no podemos decir que las redes multicast estén intrínsecamente aisladas.

Los mensajes GOOSE, a pesar de no tener ningún mecanismo de seguridad, pueden preservarse mediante técnicas de configuración de red Ethernet y manipulación del flujo de información. Utilizando una ingeniería de red correcta es posible preservar el rendimiento y la integridad de la red de datos. Aislar la red del tráfico no deseado es una buena opción de seguridad utilizando redes IEC 61850.

III. CIBERATAQUE USANDO GOOSE MESSAGING

A. Ciberataque: Vectores, Técnicas y Consecuencias

La ejecución de un ciberataque depende de tres pilares: motivación, vector y técnica. Un ataque puede estar motivado por el miedo, la demostración de la vulnerabilidad de un sistema y la especulación financiera. Los vectores son las rutas de acceso a una computadora o red. La técnica de ataque puede variar según la arquitectura de la red, la composición del marco y la dinámica de transmisión de mensajes. La técnica explorada para esta aplicación se basa en las vulnerabilidades de la capa 2 del modelo OSI (Kush, Ahmed, Branagan y Foo, 2014).

El vector puede describirse como el medio de acceso a la red informática. El acceso a la red se puede obtener a través de malware instalado en un dispositivo USB, algún equipo infectado, una persona malintencionada con acceso a la red
subestación o un hacker capaz de invadir la red de forma remota. El programa o malware no necesita tener acceso directo al equipo de publicación y suscripción. Sin embargo, debe tener la capacidad de analizar, identificar y reproducir mensajes GOOSE.

La técnica debe elegirse según el objetivo del ataque.
Debido a la naturaleza del protocolo GOOSE, es posible desarrollar técnicas capaces de explotar vulnerabilidades en la capa de enlace: VLAN Hopping, ataque de inundación MAC , ataque DHCP , ataque ARP y ataque Spoffing (Senecal, 2009). Por lo tanto, el desarrollo de la técnica exige un estudio detallado de los protocolos en cuestión.

Las consecuencias de un ciberataque dentro de una subestación pueden causar daños irreversibles a una subestación eléctrica. Los fallos en la red de datos pueden provocar un funcionamiento incorrecto de los esquemas de protección y control y un funcionamiento inadecuado de equipos primarios como disyuntores y seccionadores. Esto puede ocasionar pérdidas materiales y financieras.

B. Técnica de saturación de red con mensajes GOOSE

El escenario de prueba, Fig. 5, consta de dos IED, un conmutador administrado y una computadora para simulación de atacantes y medición de la red de datos. Los tres dispositivos se conectaron a los puertos del conmutador mediante cables de red. El conmutador se configuró de forma transparente, sin reglas ni bloqueos de puertos. Los IED funcionan con una tarjeta de red capaz de gestionar un ancho de banda de 100 mb/s.

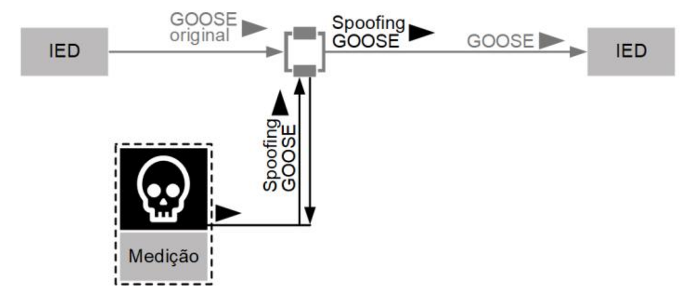


Figura 5. Escenario de prueba

Los IED fueron configurados para realizar una prueba de ping-pong. La prueba consiste en un IED transmisor que publica información booleana en la red, el IED suscriptor, al recibir la información, devuelve la respuesta a la red. El IED transmisor no firma el mensaje del IED suscriptor. El tiempo de retransmisión en estado estable es de 1000 ms y el tiempo de transmisión durante una variación es de 4 ms.

Los mensajes enviados por el malware son mensajes GOOSE clonados y manipulados del IED transmisor, consulte la Figura 6.

```
▷ Frame 9310: 1488 bytes on wire (11904 bits), 1488 bytes captured (11904 bits) on interface 0
▷ Ethernet II, Src: xxxxxxxx_0b:06:be (00:30:a7:0b:06:be), Dst: Iec-Tc57_01:00:13 (01:0c:cd:01:00:13)
◢ GOOSE
    APPID: 0x1013 (4115)
    Length: 132
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ◢ goosePdu
      gocbRef: A0401U_005_ICD_1CFG/LLN0$GO$GooseDSet15
      timeAllowedtoLive: 2000
      datSet: A0401U_005_ICD_1CFG/LLN0$DSet15
      goID: Sub1Bay1
      t: Jul  6, 2016 18:03:52.332397460 UTC
      stNum: 1234
      sqNum: 0
      test: False
      confRev: 1
      ndsCom: False
      numDatSetEntries: 1
    ◢ allData: 1 item
      ◢ Data: bit-string (4)
          Padding: 1
          bit-string: <MISSING>

◢ allData: 1 item
  ◢ Data: bit-string (4)
      Padding: 1
      bit-string: <MISSING>
```

Fig. 6. APDU generada por el malware

El datagrama GOOSE clonado fue manipulado para mantener stNum y sqNum con valores fijos y cargar los datos con bytes de relleno, sin influir así en la decisión lógica del IED.

C. Perfil de comunicación de saturación de red para el 40% Cargando

El experimento tiene como objetivo analizar el rendimiento del IED del suscriptor durante una condición de tráfico GOOSE intenso. El malware es responsable de generar el tráfico. Los paquetes fueron manipulados para no interferir con la decisión lógica del IED.

La figura 7(a) muestra el perfil de los mensajes GOOSE antes y durante el inicio del ataque de saturación. El ataque comienza entre los 10 s y los 20 s.

La figura 7(b) muestra el comportamiento del IED receptor. Los mensajes se repiten a una frecuencia constante de 1000 ms, el atributo stNum permanece constante y solo se incrementa el atributo sqNum .

La figura 7(c) representa los paquetes GOOSE enviados por el malware, el contador stNum se estableció en un valor fijo y el parámetro sqNum en cero. La tasa de envío se controló hasta alcanzar un valor de 40 Mbps, lo que representa un mensaje cada 400 μs aproximadamente.

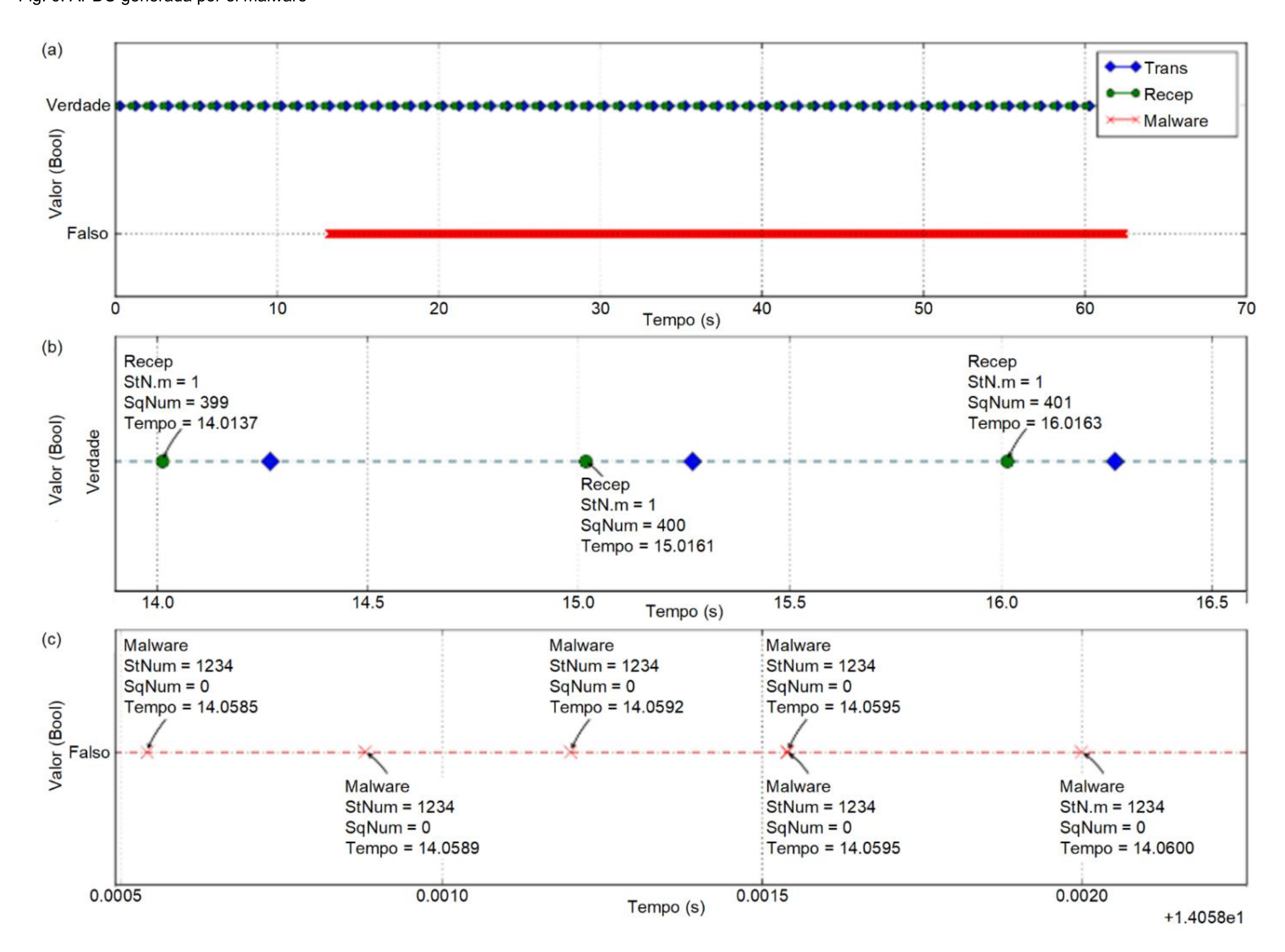


Fig. 7. Perfil de comunicación de GOOSE antes y durante el ataque (a); Perfil de comunicación de GOOSE durante el ataque (b); Perfil de comunicación de malware durante el ataque (c)

La figura 8 muestra el ancho de banda utilizado durante el ataque. Durante la operación previa al ataque, el ancho de banda utilizado por la red es de aproximadamente 2 Kbps. Durante el ataque, el ancho de banda registrado fue de 40 Mbps, debido a la carga generada por el malware.

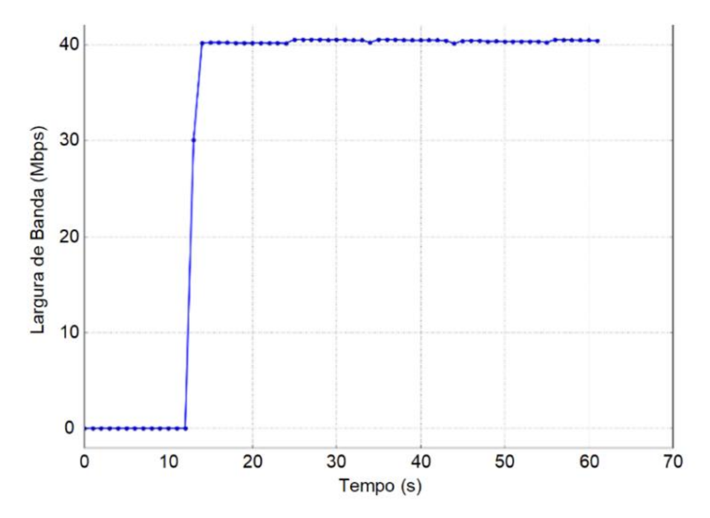


Fig. 8. Ancho de banda de 40 Mbps registrado durante el ataque

Al iniciar el ataque, el IED receptor identifica que se está enviando un mensaje fuera de secuencia y un mensaje corrupto. El mensaje fuera de secuencia se reconoce debido al parámetro stNum del malware, establecido en un valor fuera de la secuencia natural del IED transmisor. El IED receptor identifica que la información contenida en la APDU no es esperada por el algoritmo de recepción y la descarta. Después de descartar el mensaje, el algoritmo de recepción asume que el siguiente mensaje es la nueva secuencia válida. El perfil de comunicación de los mensajes GOOSE durante esta simulación de ataque fue satisfactorio y no se observó pérdida de paquetes.

D. Perfil de comunicación de saturación de red para el 85% Cargando

El ataque continúa con el malware aumentando la tasa de transmisión de los mensajes GOOSE, hasta alcanzar un nivel de 85 Mbps.

La figura 9(a) muestra el perfil de los mensajes GOOSE durante el ataque de saturación. El ataque comienza en el instante 0. La tasa de envío del malware fue controlada hasta alcanzar un valor de 85 Mbps, lo que representa un mensaje cada 190 µs aproximadamente.

La figura 9(b) muestra 2 paquetes que pertenecen al receptor. El parámetro stNum se mantuvo constante en ambos paquetes, lo que indica que pertenecen al mismo orden de variación. sqNum se incrementó en 1 durante un intervalo de 1000 ms . Sin embargo, el mensaje del transmisor no fue grabado hasta que transcurrieron 5 segundos.

La figura 9(c) representa un paquete perdido por el receptor en el tiempo 9.5.

Fig. 9. Ataque GOOSE para 85% de ancho de banda (a); pérdida de paquetes del IED transmisor (b); pérdida de paquetes por el receptor (c)

La figura 10 representa el ancho de banda de 85 Mbps. grabado durante el ataque.

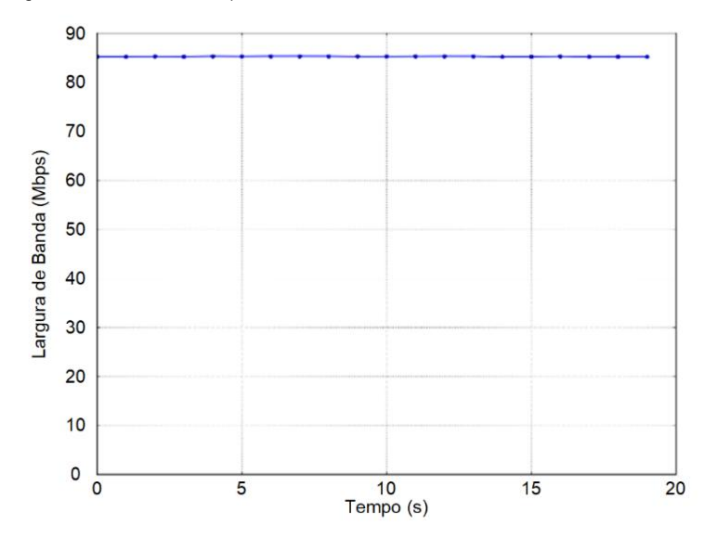


Fig. 10. Ancho de banda de 85 Mbps registrado durante el ataque

Los IED continuaron registrando mensajes fuera de secuencia y corrompiéndolos. Sin embargo, fue posible verificar el aumento de mensajes perdidos debido a la saturación del receptor, demostrado por la pérdida de paquetes del receptor y del transmisor. El perfil de transmisión quedó claramente dañado debido al aumento de tráfico inyectado por el malware. Por lo tanto, es posible concluir que la red ya no es confiable para el tráfico de ningún tipo de mensaje o medición de datos en esta situación, exponiendo la vulnerabilidad de la red.

IV. CIBERSEGURIDAD PARA SUBESTACIONES ELÉCTRICAS

A. Gestión de capa 2 mediante etiquetas IEEE 802.1Q

Las subestaciones modernas ofrecen facilidades y mejoras en la implementación de funciones utilizando la red de comunicaciones. Cuando se implementan de forma segura, ofrecen confiabilidad y eficiencia. Sin embargo, si se implementan de forma incorrecta y con brechas de seguridad, pueden ofrecer vulnerabilidades a ataques y fallos en el sistema de automatización, reduciendo la confiabilidad y eficiencia de la instalación (Ewing, 2010).

Las redes de área local virtuales (VLAN) son redes particionadas y aisladas en la capa de enlace de datos del modelo OSI.
Las VLAN utilizan tecnología IEEE 802.1Q que define la estandarización del sistema de etiquetas sobre la trama Ethernet (IEEE Std. 802.1Q, 2012). La figura 11 muestra un esquema del tráfico de mensajes gestionado por el conmutador.
Utilizando etiquetas IEEE 802.1Q en tramas Ethernet es posible gestionar el flujo de datos a través de la capa de enlace del modelo OSI.

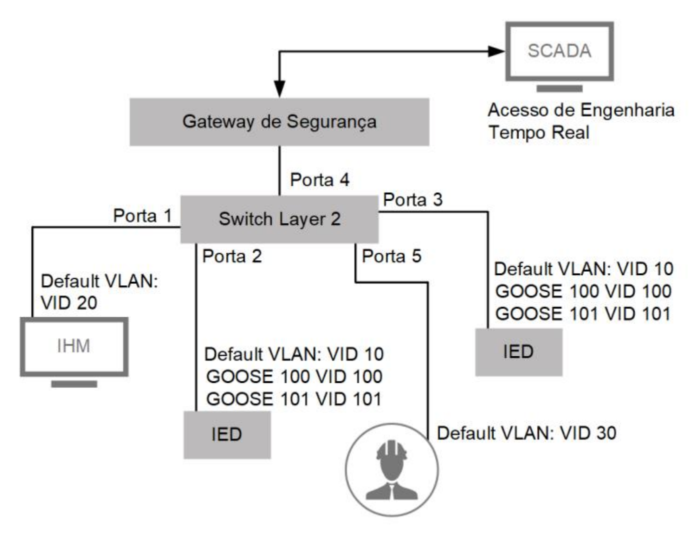


Fig. 11. Diagrama de red utilizando VLAN

El acceso entre VLAN ID 10, 20, 30 se realiza a través del Security Gateway y un firewall administra la inspección de paquetes y los niveles de acceso. Por lo tanto, el flujo de información con las etiquetas 10, 20, 30 se dirige al puerto 4 y se distribuye a los puertos de interés y al sistema SCADA. Las VLAN 100 y 101 son específicas de los mensajes GOOSE y no requieren enrutamiento a través del enlace de seguridad. Los mensajes GOOSE viajan exclusivamente a través de los puertos 2 y 5. Por lo tanto, sólo los dispositivos de interés comparten la información.

La gestión de red mediante VLANS permite aislar la red de datos sólo para aquellos dispositivos de interés, dificultando el acceso a personas no autorizadas y optimizando el rendimiento de la red de comunicaciones ya que se divide el tráfico multicast.

B. Red definida por software: SDN

SDN es una arquitectura de red estática basada en tecnología de tabla de búsqueda, es ideal para el rendimiento de la red al reducir el ancho de banda a través del control de flujo de software. SDN es un enfoque que utiliza protocolos abiertos, como OpenFlow, que permiten el control de flujo en equipos de borde como conmutadores (Open Networking Foundation, 2016).

La arquitectura SDN tiene 3 niveles: Aplicación, controlador de flujo e infraestructura de red. La figura 12 muestra la interacción entre los 3 niveles. La capa de aplicación tiene 3 funciones principales: Operación, administración y gestión del sistema (OAM). El controlador de flujo es la aplicación central que permite la visualización de la red e instruye al sistema sobre cómo manejar los paquetes. La infraestructura de red es el equipo que recibe instrucciones del controlador y dirige los paquetes a sus respectivos destinos.

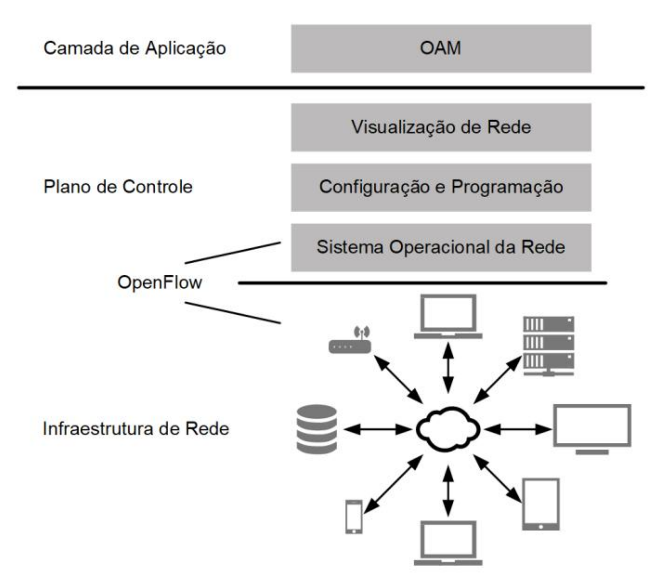


Figura 12. Arquitectura de red SDN

OpenFlow utiliza valores contenidos en una tabla de verdad para controlar el flujo a través de la red y para el procesamiento interno de la conmutación. Una entrada de tabla de verdad contiene información presente en el encabezado del mensaje. Para los mensajes GOOSE, las entradas de la tabla de verdad pueden ser cualquier información del encabezado Ethernet, como la etiqueta IEEE 802.1q o la dirección MAC de destino.

El conmutador compara las entradas adquiridas con cada entrada en la tabla de verdad buscando una regla válida. Luego, el paquete se aplica a la salida de la acción y el conmutador reenvía el paquete al puerto especificado o descarta el mensaje.

Una vez realizada la ingeniería de la red SDN, el switch se comportará según lo configurado por el usuario, eliminando posibles rutas de invasión y sobrecarga de la red de datos. Las redes SDN representan un gran avance en seguridad y rendimiento en las redes de subestaciones.

V. CONCLUSIÓN

La norma IEC 61850 ofrece interesantes características para la automatización de subestaciones eléctricas. Los mensajes GOOSE se pueden utilizar para compartir señales de bloqueo, apertura y cierre de equipos dentro de un SE. Debido al alto requisito de rendimiento, los procedimientos de autenticación y seguridad se abstraen de la dinámica de transmisión, lo que hace que los mensajes GOOSE sean intrínsecamente vulnerables. Técnicas de ataque como: manipulación de tramas Ethernet y saturación de la red de datos, pueden comprometer el desempeño de los equipos involucrados en el sistema de protección y control. Las mejores prácticas para configurar redes Ethernet y nuevas tecnologías como la gestión de red basada en software (SDN) pueden minimizar el riesgo de ataques y aumentar el rendimiento de la red de datos.

Los mensajes GOOSE están definidos por IEC 61850-8-1 y asignados al marco Ethernet. La APDU tiene una serie de parámetros que se utilizan para el análisis de errores y la recepción de datos. Los IED pueden utilizar parámetros como stNum y SqNum para comprobar y procesar mensajes GOOSE. Sin embargo, sin un mecanismo para autenticar la fuente del mensaje, estos parámetros de confirmación pueden enmascararse fácilmente y usarse con fines maliciosos.

La técnica de saturación de la red de datos, explorada en este artículo, mostró cómo la dinámica de transmisión de multidifusión puede utilizarse de forma maliciosa e influir en el rendimiento de los equipos conectados a la red de datos. Al llegar a un límite cercano a la capacidad de datos, fue posible observar pérdida de paquetes tanto de los equipos, transmisor como receptor. La red de datos se ha visto comprometida debido al ataque y ya no se puede garantizar la entrega de paquetes.

Las mejores prácticas de red se pueden utilizar para mitigar posibles ataques y garantizar la integridad del intercambio de mensajes. El uso de la tecnología IEEE 802.1Q garantiza la segregación de redes en la capa de enlace mediante la configuración de switches y la inserción de etiquetas en las tramas Ethernet. Las redes SDN son ciberseguras por diseño tecnológico. La topología estática de las redes SDN permite un acceso preciso y un control de flujo en los puertos de los controladores de red, evitando así cualquier forma de ataque dentro de las subestaciones.

VI. REFERENCIAS

[1] D. Dolezilek, D. Whitehead y V. Skendzik, "Integración de IEC 61850 GSE y servicios de valor muestreado para reducir el cableado de subestaciones", actas de la 12.ª Conferencia Anual de Automatización de Suministro de Energía Occidental, Spokane, WA, abril de 2010.

[2] C. Ewing, "Ingeniería de ciberseguridad de defensa en profundidad para la subestación moderna", actas de la 12.ª Conferencia Anual de Automatización del Suministro de Energía Occidental, Spokane, WA, abril de 2010.

[3] J. Hoyos, M. Dehus y T. Brown, "Explotación del protocolo GOOSE: un ataque práctico a la ciberinfraestructura", actas de los talleres IEEE 2012 Globecom, Anaheim, CA, diciembre de 2012.

[4] K. Zimmerman, "Recomendaciones de SEL sobre pruebas periódicas de mantenimiento de relés de protección", marzo de 2014. Disponible en: https:// selinc.com.

[5] IEC 61850-5, Redes y sistemas de comunicación en subestaciones – Parte 5: Requisitos de comunicación para funciones y modelos de dispositivos.

[6] IEC 61850-8-1, Redes y sistemas de comunicación en subestaciones – Parte 8-1: Mapeo de servicios de comunicación específicos (SCSM) – Asignaciones a MMS (ISO 9506-1 e ISO 9506-2) y a ISO/IEC 8802-3, 2004.

[7] Estándar IEEE 802.1Q, Puentes de control de acceso al medio y redes de área local con puentes virtuales.

[8] J. Konka, C. Arthur, F. Garcia y R. Atkinson, "Generación de tráfico de valores muestreados IEC 61850", actas del Primer Taller Internacional IEEE sobre Modelado y Simulación de Redes Inteligentes (SGMS), Bruselas, Bélgica, octubre de 2011.

[9] C. Kriger, S. Behardien y J. Retonda-Modiya, "Un análisis detallado de la estructura del mensaje GOOSE en un sistema de automatización de subestaciones basado en el estándar IEC 61850", International Journal of Computers, Communications & Control (IJCCC), vol. 8, número 5, octubre de 2013, págs. 708-721.

[10] N. Kush, E. Ahmed, M. Branagan y E. Foo, "Poisoned GOOSE: Exploiting the GOOSE Protocol", actas de la Duodécima Conferencia Australasiana de Seguridad de la Información, Auckland, Nueva Zelanda, enero de 2014.

[11] L. O'Fallon, D. Klas, T. Tibbals y S. Shah, "Optimización de red SCADA MMS IEC 61850 para IED", actas de la Conferencia DistribuTECH, San Diego, CA, febrero de 2011.

[12] Open Networking Foundation, "OpenFlow", consultado el 1 de agosto de 2016. Originalmente disponible en https://www.opennetworking.org/sdn-resources /flujo abierto.

[13] C. Ozansoy, Modelado e implementación orientada a objetos de IEC 61850: El nuevo estándar internacional sobre comunicación y automatización de subestaciones, Lap Lambert Academic Publishing, 2010.

[14] L. Senécal, “Comprensión y prevención de ataques en la capa 2 del modelo de referencia OSI”, actas de la 4ª Conferencia Anual de Investigación sobre Redes y Servicios de Comunicación, mayo de 2006.

[15] Wireshark, accedido julio 1º, 2016. Disponible en https://www.wireshark.org/.

VII. DATOS BIBLIOGRÁFICOS

Mauricio Gadelha da Silveira nació en Monte Aprazivel, SP, el 29 de enero de 1988. Se graduó en Ingeniería Eléctrica por la Universidade Estadual Paulista (UNESP) en 2013. Actualmente forma parte del equipo de Ingeniería y Servicios de Schweitzer Engieering Laboratories (SEL), donde ocupa el cargo de Ingeniero de Protección.

Paulo Henrique Franco nació en Piracicaba, SP, el 3 de marzo de 1981. Se graduó en Ingeniería Eléctrica por la Universidad Estadual Paulista (UNESP) en 2004. Actualmente forma parte del equipo de Sistemas de Protección Especial de SEL Engieering Services (SEL-USA), donde ocupa el cargo de Ingeniero de Automatización.

20210302 • TP6974-01